International Journal of Management (IJM)
Volume 7, Issue 5, July–Aug 2016, pp.173–182, Article ID: IJM_07_05_016
Available online at
http://www.iaeme.com/ijm/issues.asp?JType=IJM&VType=7&IType=5
Journal Impact Factor (2016): 8.1920 (Calculated by GISI) www.jifactor.com
ISSN Print: 0976-6502 and ISSN Online: 0976-6510

DEVELOPMENT OF CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION: A CASE STUDY OF THAILAND

Settapong Malisuwan
National Broadcasting and Telecommunications Commission (NBTC), Thailand

ABSTRACT

Nowadays, critical infrastructures such as systems of water supply, electricity, public transportation, irrigation, public healthcare and banking adopt various information systems as a part of its functions and it will become essentially needed in the future because these public services will be accessible by people via the internet. As a result, governments in many countries consider it as a priority to provide their people with easy and convenient internet access because it will bring many positive impacts to the country development in all aspects such as the government sector, private business sector, civil sector and specifically the nation to be able to increase its competitive capability. However, easy internet access may lead to potential cyber risks, meaning that the level of cyber protection will be decreased and cybercrime may happen without difficulty. Therefore, the cyber security has become a top priority for critical infrastructures. This paper proposes a guideline to develop measures to handle cyber attacks and to enhance ability to prevent and recover from cyber threats in order to make cyberspace secure and sustainable. A case study of Thailand's national plan for critical infrastructure protection is presented in this research. The research method is qualitative in-depth interview with many experts in various fields. Inputs of secondary data are analyzed from academic papers, business and best-practices reports made by respectable reference sources. The contributions in this paper could assist governments in development of cybersecurity to protect and foster the digital economy.

Key word: Cybersecurity, Critical Infrastructure, Development, Thailand

Cite this Article: Settapong Malisuwan, Development of Cybersecurity and Critical Infrastructure Protection: A Case Study of Thailand. *International Journal of Management*, 7(5), 2016, pp. 173–182.
http://www.iaeme.com/IJM/issues.asp?JType=IJM&VType=7&IType=5

1. INTRODUCTION

Rapid development of Information and Communication Technology highly increases data analytical capabilities of individual and organizations to become faster than ever before. Network connectivity has completely changed a concept of business model and thinking process. A new phenomenon is happened i.e. more tangible organizational assets turn to intangible assets. By this, the Cyber Ecosystem becomes more important and it makes the communication society of human become faster and more complicated by adopting network technologies for connection until there are no more obstacles of time and locations.

Cyber helps overcome barriers of communication and business processes. Information can be exchanged rapidly with only one-finger touch which produces advantages to the human being in developing their economy and societies. However, a coin has two sides; even cyber has a number of benefits, it also leads to cyber threats in the same time such as privacy violations, espionage etc. These cyber threats can affect to potential collapses of the economy, society and security in the nation [1].

Countries and organizations still need to adopt cyberspace in creating competitive advantages and getting the most out of it at the highest risk. As a result, each country and organizations have to adjust themselves to cyber incidents, threats, and challenges by increasing their capabilities in Resistance, Reaction and Recovery by all means trying to violate their cybersecurity, including developing their capabilities on reducing potential risks from cyber attacks.

Today, cybersecurity development has been much more changed comparing from yesterday. In previous days, information was mostly exchanged among relevant people inside organizations, but nowadays it is different. A number of organizational information are disseminated and shared with others, including customers. Also, some staffs have to work on-site, it then becomes more complex to increase the Cybersecurity. Consequently, sufficient development of critical infrastructure protection and personnel capabilities are required to respond to any complicated cyber threats both inside and outside the organizations which require cooperation from all relevant stakeholders [2].

To achieve the objective of this research, this paper is organized as follows. Section II explains the research methodology. Section III presents a guideline for the establishment of measures to handle cyber threats. A case study of Thailand's national plan for critical infrastructure protection is introduced in section IV. The conclusion is provided in the last section.

2. RESEARCH METHODOLOGY

The objectives of this research is to propose a guideline to develop measures to handle cyber attacks and to enhance ability to prevent and recover from cyber threats. It is intended as a qualitative research based on in-depth interviews and supported by inputs of secondary data called from academic papers, business and best-practices reports made by respectable reference sources. Its primary data will come from in-depth interviews of distinguished experts in related fields under the following research framework as illustrated by Fig.1.

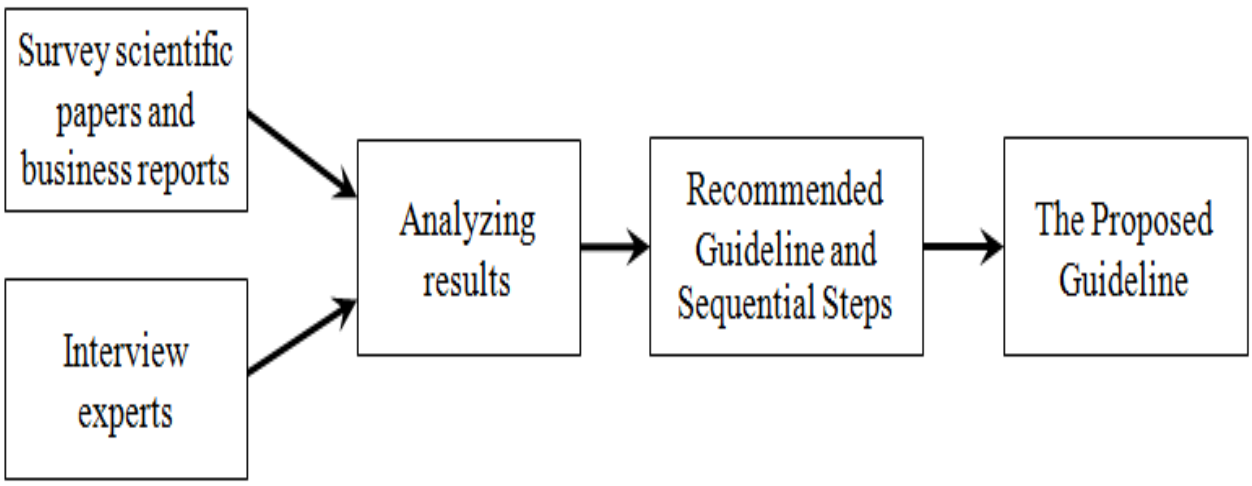

Figure 1 Research framework

The respondent profiles of our subject matter experts are shown in Table 1. We classified subject matter experts into four categories depending on their area of expertise in Telecommunications, Economics, Strategic Management, and Cybersecurity. The total number of subject matter experts or respondents is 12 with 3 from each key focus area.

Table 1 Interviewing Experts and Key Focus

Area of expertise	Numbers
Telecommunications	3
Economics	3
Strategic Management	3
Cybersecurity	3

Inputs from the in-depth interviews will be processed and analyzed together with secondary data which will be summarized into a preliminary draft conclusion to be forwarded to the 12 experts for further comments with an intention of streamlining them into a shared common direction. The version assessed and scrutinized by the 12 experts will then be adopted as a basis for formulating a guideline for implementing key points to ensure efficient and successful cybersecurity development.

3. GUIDELINE FOR ADJUSTMENTS TO CYBER ENVIRONMENT

The establishment of measures to handle cyber attacks should be well adjusted to the cyber environment and enhance its ability to prevent and recover from cyber threats in order to make cyberspace secure and sustainable [3],[4],[5].

1. Government Measures

Government Units and concerned organizations will have to increase the security levels of maintenance management data and information systems. Moreover, the preparedness against cyber-attacks needs to be enhanced as well.

- Guidelines for improving the security of data and information systems.

The creation of strengthening measures for the government information systems to be more efficient, especially for the fundamental infrastructure of government information systems in order to adjust cyber attacks and severe disasters by applying the followings; 1) Change information systems into Cloud Services Standards, 2) Promote information sharing fundamental infrastructure with other systems concerned which are managed and operated by government sectors, local authorities and other authorities related to fundamental structures, 3) Implement measures for the operation and ensure that those measures can secure data of e-government systems.

The determination of technical standards for the security systems for the government information system, the results of technical standard implementation as well as enhancement of existing measures to be more potential should be monitored and evaluated within the scope of international agreements, or in compliance with the international standards and all necessary measures for national security. And data security measures will also require closed cooperation and collaboration.

If the private sector gets involved in significant information security, this may bring more efficiency than government sector working alone. The conditions to secure significant data must be certified by external organization which has standards of operation to support the internal operations. Moreover, it is necessary to support the state agency in charge of cyber security to present the report of the situations on cyber attacks and the use of data jointly between entrepreneurs. Therefore, it is necessary to set an operational framework for the utilization of specific risk assessment.

Independent agency in charge of government cyber security or organization under government control will have more efficient measures for data security. Nevertheless, while performing their duties, they have to be aware of cyber attacks. Reports will have to be made as legally or intentionally required to the government agency in charge of security on threatening situations as well as on the use of data jointly with other concerned government agencies in order to prevent any damages from spreading more.

- Preparation for effective handling of cyber attacks

The development of cognitive and analysis ability of cyber attacks and measures to handle cyber threats of government sector may be different from previous ones due to more severe threats nowadays. For example, Japanese government has established the Government Security Operation Coordination team or GSOC for monitoring situations, preparing operational framework of technology for gathering and analyzing occurring treats, and providing a system used to analyze the results caused by cyber attacks. Moreover, the system should be developed for data sharing and analysis of existing treats with government sector and agencies related to critical infrastructures.

Regarding the operation of cyber security resulting from the cooperation between the government and any other concerned agencies related, such as the cooperation between GSOC, CYMAT (Cyber Incident Mobile Assistant Team) and the agency whose duty is to respond to the threatening situations during the time when cyber treats arise. So, each agency must immediately share and exchange information of existing cyber treats and also provide a complete Preparedness System for handling cyber attacks and setting measures for handling possible cyber attacks. For examples, organizing the training of preliminary handling methods for cyber treats, and proceeding systematically data collection and classification with effective preparedness in order to get effective handling method. This action must require cooperation between the government sector and other concerned agencies.

Moreover, the government's ability to manage situations for both normal or emergency ones will require human resources support, and cooperation between countries by conducting a training for personnel of each government sector for their ability to respond to such threats quickly and accurately, or by conducting the exchange of personnel between government sector and private sector.

2. Measures Provided by Critical Infrastructures Service Providers

The critical infrastructures are necessary in our daily lives as they facilitate all activities to operate in continuous and reliable manners whether those activities are economic, social or government affairs. Therefore, information security measures are required in compliance with the operation of government to prevent possible threats as follows.

1. Measures focusing on data security for critical infrastructures service providers should include evaluation and risk analysis, have a procedure that can be adjusted based on the characteristics of the data infrastructures, which are different in each field and create a procedure that reflects the results caused by those risks through the preparation of safety standards handbooks for each field of important data organizational infrastructure.
2. Providing support to information about the failure, cyber attacks, existing cyber threats and defects between major infrastructures service providers, data exchange and analysis systems in the authorities relevant to major infrastructures. However, bringing information about existing targeted attacks in different industries to mutually use may be hard to do. Therefore, a mutual agreement on protecting confidentiality measures of sharing information is required to set up. Those measures must be developed and widely adopted.
3. Encouraging different infrastructures service providers of each field, entrepreneurs relevant to cyberspace and any other concerned organizations to be capable of cooperating to respond to cyber attacks. Those service providers should prepare reports to ministry or authorized agency immediately after cyber-attacks that require data exchange with concerned parties, managing personal confidential information procedure as well as cybersecurity procedure between critical infrastructures service providers.
4. Regarding risk management for critical infrastructures, it is necessary to conduct Information Security Assessment/Assurance Program, to encourage critical infrastructures service providers and entrepreneurs relevant to cyberspace to work and to share information together. The defined agency in charge of monitoring Information Security Assessment Audit/ Assurance Program in compliance with international standards is appointed.
5. Establishing measures responding and counterattacking cyber attacks, such as conducting personnel training, and gathering normal data and unexpected data to facilitate government sector and private sector to work together and implement appropriate measures in case of cyber-attacks. Moreover, efficient responding

measures to cyber attacks are already prepared, such as organizing handling the training courses for severe cyber attacks to related agencies or adaptation of referencing case studies from other countries if necessary.

3. Measures in the Private Sector, Educational institution and Research Institute

In case of any mutual use of information sharing among private company, educational institution and research institute, this will improve the ability to identify and analyze the cyber attacks more efficiently that can help to manage important information, such as trade secrets, confidential business information, intellectual property information, and personal information which are the sources of international competition's ability. Therefore, private company, educational institution and research institute should adopt cybersecurity measures as follows:

1. In small to medium- sized organization where the experts for cyber may be not available and there are not adequate investments to handle with cyber attacks. Therefore, efficient environmental management for handling cyber attacks is required, especially data exchange systems must be provided to give consultation between small to medium sized entrepreneurs medium-sized organization, tax systems with data security, such as available audit, handbook and easy tools used to develop and improve data security, change for better data security, i.e. cloud computing technology.
2. Encouraging an analysis of the information about occurring situation in small to medium sized enterprises, such as a mutual adoption of cyber treats defensive measures among enterprises, practical for cyber defense, and usability of practical test that are not only implemented to medium sized enterprise but also small-sized enterprises and retail operators should also adopt them to use in order to improve abilities to respond, handle and manage cyber attacks.
3. Providing support to establishment of agencies in charge of responding to treat notification of each organization to improve abilities to respond to existing treats and to prevent invasion of damages in private company, educational institution, research institute and other concerned organization. Then, ensuring that the agencies in charge of responding to treat notification of each organization can work together effectively.
4. Dissemination and education administration related to information security should be promoted to be included in the curriculum of educational institutions in order to optimize and develop the quality of the educational activities by using and applying continuously information technology resulted from an increase of information in educational systems.

4. THAILAND'S NATIONAL PLAN FOR CRITICAL INFRASTRUCTURE PROTECTION PROJECT: A CASE STUDY

To achieve the design of cybersecurity policy, one way to begin is to break all the national interests that might be essential to the survival and wellbeing of the nation into three main categories [6]: (1) interests related to our security as a nation; (2) interests related to our economic health as a nation; (3) interests related to the core values and beliefs that define our nation. Table 2 demonstrates the national interest chart of cybersecurity.

Table 2 National Interest Breakdown Chart for Cybersecurity: A Partial List

Security Interests	• protecting national critical information infrastructure • ensuring the safety of citizens from harm by foreign attackers • protecting military information infrastructure • preventing foreign intrusions into national critical information infrastructure • maintaining military power to protect national cybersecurity interests • maintaining knowledge regarding potential threats to national cybersecurity
Economic Interests	• protecting and/or promoting an adequate ICT services for domestic citizens • ensuring economic development and growth by digital economy policy • protecting the competiveness of key domestic ICT industries • maintaining ICT power to ensure economic self-determination
Ideological Interests	• protecting and/or promoting a moral way of life in cyber • protecting and/or promoting a moral cyber economic system • protecting and/or promoting the cultural and/or religious values of a nation or a people through cyber • advancing and protecting a universal conception of freedom, justice, progress and/or human dignity through cyber

A definition of Critical Infrastructures may be varied and cannot be used as a single definition for the same understanding across the world. So, this document will adopt the frequently-used definition of critical infrastructures i.e. essential services that underpin the country society and if these basic services do not function properly or cannot provide regular services, even in a short period of time, it will cause vast negative impacts to industrial sectors or a particular organization. Moreover, these effects will broadly affect to a group of people' security and safety in term of society and economy. A group of people can be a country's population or people in a group of countries that are affected by its negative expansion.

The cyber attacks do not aim to create negative impacts to communication networks only, but it can expand its effects to other types of critical infrastructures. These attacks will cause serious negative impacts to the national security in term of human well-being, life and property. Some negative examples are the following: people cannot make their banking operation successfully, basic infrastructure services are not working, patients cannot access to their public healthcare because of no patients' records, or even the public transportation system is stopped for a short period of time, it can damage the social stability and socioeconomic welfare of the nation in a minute [7].

Current situation of Thailand

The International Telecommunication Union or ITU, who is a UN agency for information and communication technologies, considers it as critical issues. In the year 2007, a framework on Global Cybersecurity Agenda (GCA) was established in order to enhance international cooperation among countries become secured in the cyber information society. Since its launch, the GCA has attracted cybersecurity experts around the world. GCA has established five key strategic pillars for cybersecurity as follows:

1. Legal Measures
2. Technical & Procedural Measures
3. Organizational Structures
4. Capacity Building
5. International Cooperation

In the year 2014, ITU initiated the Global Cybersecurity Index (GCI) which is the multi-stakeholder initiative to measure the commitment of countries to cybersecurity. Thailand ranked 15 of 29 in the world and ranked 7 of 15 in Asia Pacific [8]. Anyhow, this ranking of GCI was based on other sources of information because it was the first year to conduct the assessment. It was expected that after that year, GCI would develop its assessment standard to become one of top acceptable indicator tools on cybersecurity to be adopted in many countries. Thailand gained only half scores or less on each key strategic pillar, meaning that Thailand should improve its measures on the cybersecurity because it will affect the strategy on becoming a regional Hub of the information system. The Asia Pacific region ranking is demonstrated in Table 3.

Thailand's ICT technology has developed continuously, considered at the higher level compared with those of other ASEAN countries. In relation to this, the ITU has revealed the annual survey results regarding ICT-society indices or "Measuring the Information Society Report (MIS Report)" which is published annually. The ITU MIS report 2015 identified Thailand as one of a group of "most dynamic countries" that recorded above-average improvements in their IDI ranking over the past five years, supported mainly by improvement in mobile broadband penetration [8],[9].

Table 3 Asia Pacific region ranking by index

Asia Pacific	Index	Regional Rank
Australia	0.7647	1
Malaysia	0.7647	1
New Zealand	0.7353	2
India	0.7059	3
Japan	0.7059	3
Republic of Korea	0.7059	3
Singapore	0.6765	4
Hong Kong	0.6176	5
Indonesia	0.4706	5
China	0.4412	6
Mongolia	0.4118	7
Sri Lanka	0.4118	7
Thailand*	0.4118	7
Brunei Darussalam	0.3824	8
Myanmar	0.3824	8
Philippines	0.3529	9
Viet Nam	0.3235	10
Bangladesh	0.2941	11
Iran	0.2941	11
Afghanistan	0.2647	12
Pakistan	0.1765	13
Samoa	0.1765	13
Vanuatu	0.1471	14
Bhutan	0.1176	15
Cambodia	0.1176	15
Micronesia	0.1176	15

Having the National Plan for Critical Infrastructure Protection will significantly imply to the GCI assessment because it is one of the core factors to ensure of being the regional Information System Hub [10]. Cyber system plays an important role in many aspects. If the country does not have the National Plan for Critical Infrastructure Protection in place, it cannot ensure other international cyber communities that Thailand can be a safe regional Information System Hub for their business operation.

Implementation of the National Plan for Critical Infrastructure Protection

At present, some initiative actions were made such as the seminar on "Cyber Incident Simulation and Conference on National Critical Infrastructure Protection" was organized in collaboration with the Ministry of Defence, NBTC and ITU in Thailand. Table 4 shows the action plan of the assessment of critical infrastructure as a result of the conference.

Table 4 Action Plan

	Phase 1	**Phase 2**	**Phase 3**
Duration:	**6 months**	**3 months**	**3 months**
Expected Outcome:	Assessment of Thailand Cybersecurity, including suggestions provided for the strategic plan development on National Plan for Critical Infrastructure Protection.	Assessment result of phase 1 including the exploration of collaborative cooperation with other relevant agencies, suggested in the phase 1will be the performance indicators.	Assessment result in phase 2 will be the performance indicators.

Phase 1: National Cybersecurity Assessment

It will assess in term of both quality and quantity in protecting critical infrastructures by considering the nation's security strategies as top priorities. The five key pillars will be assessed as the following:

Legal Measures: assess measures and regulations on the national critical infrastructure protection by considering two sub-topics as below:

- Cybercrime legislation
- Regulation and compliance

Technical & Procedural Measures: Technologies are the first priority to use protecting any cyber attacks and managing cyber crimes. On this topic, technologies of relevant agencies on cybersecurity will be assessed whether they have efficient technologies and operations by considering the following sub-topics:

- CERT/CIRT/CSIRT
- Standards
- Certification

Organizational Structures: responsible organizations will need to initiate its strategic plan and actions. The assessment will focus on a number of existing organizations along with their cyber protection strategies including their development at national level. The following sub-topics will be assessed:

- Policy
- Roadmap for governance
- Responsible agency
- National benchmarking

Capacity Building: it is by-products from the assessment of Legal, Technical and Organizational Structures. It will include awareness building and sufficient available resources. Moreover, it will assess research & development, learning and training including existing experts on this issue in each organization. Here below are the sub-topics to be assessed:

- Standardization development
- Manpower development
- Professional certification
- Agency certification

International Cooperation: Cybersecurity and Protection require participation from many stakeholders in an essence of cooperation, discussion and implementation which will contribute to high performance. The cooperation can be made both locally and internationally. The sub-topics to be assessed are as follows:

- Intra-state cooperation
- Intra-agency cooperation
- Public-private partnerships
- International cooperation

Phase 2: The National Critical Infrastructure Protection Framework Development will adopt the assessment result from phase 1 to develop a framework of the national plan.

Phase 3 The National Cybersecurity Drill and Human Capacity Building will increase capability and capacity of all relevant personnel at both the organizational level and individual level in order to respond to the national plan.

5. CONCLUSION

Currently, organizations cannot operate their business without connection with others. So, only internal measures of the cybersecurity management are not enough secured for the whole organizations. Then, it is necessary for the organizations to invest on efficient cybersecurity technologies within the organizations themselves as well as co-investing with their partners. Then, it is essential that business firms need to broaden their collaborative ranges more than yesterday. Today, it is not enough to only perform the threat-monitoring, but closely working in collaboration with connected partners is needed either they are in the same industries or they are competitors including governmental sectors. The government and cybersecurity-driven organizations play major roles in establishing policies and frameworks to drive the development of the Cyber Resilience which is not easy to implement, but it is the must to make it success in order to create sustainable security for the country.

REFERENCES

[1] Cyber Risk - A Global Systemic Threat, White paper, DTCC, October, 2014.

[2] Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, Cyber Security and the UK's Critical National Infrastructure, Chatham House Report September 2011.

[3] Cybersecurity, Internal Report, NBTC, Thailand, Dec. 2015.

[4] F. Wamala, ITU National Cybersecurity Strategy Guide, *International Telecommunication Union* (ITU), Geneva, September 2011.

[5] Get Ahead of Cybercrime, Ernst and Young, 2014.

[6] National Interest and Tools for Foreign Policy, Close up Foundation, Washington DC., 2013.

[7] The National Strategy to Secure Cyberspace, The White House Washington, Febuary 2003.

[8] Measuring the Information Society Report 2015, International Telecommunication Union (ITU), Geneva, 2015

[9] Guidelines for the Preparation of National Wireless Broadband Master Plans for the Asia Pacific Region, International Telecommunication Union (ITU), October 2012.

[10] Framework for Improving Critical Infrastructure Cybersecurity, NIST, Febuary 12, 2014.

[11] Settapong Malisuwan, Dithdanai Milindavanij and Wassana Kaewphanuekrungsi. Voice and Internet Service Charges in Asean Members: Analysis and Recommendations. International Journal of Advanced Research in Management, 7(3), 2016, pp. 01-12.

[12] Settapong Malisuwan, Noppadol Tiamnara and Dithdanai Milindavanij. The Impact of Spectrum Assignment on Economic Growth and Competitiveness in Thailand. International Journal of Management, 6(12), 2015, pp. 11-21.

[13] Settapong Malisuwan, Dithdanai Milindavanij and Noppadol Tiamnara. Thailand's International Internet Gateway (IIG): Market and Development. International Journal of Advanced Research in Management, 7(1), 2016, pp. 24-33.

[14] Settapong Malisuwan, Dithdanai Milindavanij and Noppadol Tiamnara. Telecommunications Regulatory Policy on Research and Development in Thailand, International Journal of Industrial Engineering Research and Development, 7(1), 2016, pp. 1–9.

[15] Settapong Malisuwan, Dithdanai Milindavanij and Noppadol Tiamnara. Telecommunications Business Transformation: Framework and Recommendations. International Journal of Management, 7(1), 2016, pp. 50-60.

[16] Settapong Malisuwan and Wassana Kaewphanuekrungsi, Technological Factors Promoting The Expansion of Internet of Things. International Journal of Advanced Research in Engineering and Technology, 7(2), 2016, pp. 21-29

[17] Shatha. A. Sameh and Hiba .K. Ismaeel, The Effect of LSM Corrosion Protection on Al Alloys. International Journal of Advanced Research in Engineering and Technology, 7(1), 2016, pp. 17-29.

[18] Settapong Malisuwan, Jesada Sivaraks, Dithdanai Milindavanij and Wassana Kaewphanuekrungsi. Development of Mobile Financial Services In Thailand. International Journal of Management, 7(1), 2016, pp. 15-25.

[19] Ninlawan Petchraburanin, Settapong Malisuwan, Dithdanai Milindavanij and Wassana Kaewphanuekrungsi, Broadband Telecommunications Infrastructure in Thailand: Analysis and Recommendations. International Journal of Management, 7(4), 2016, pp.142–151.

[20] Settapong Malisuwan and Dithdanai Milindavanij. Balancing Social Benefits and Market Competition in Thailand's Mobile Telecommunications Industry: Regulatory Perspective. International Journal of Information Technology & Management Information System, 7(1), 2016, pp. 18–27.

[21] Ninlawan Petcharaburanin, Settapong Malisuwan and Dithdanai Milindavanij, Analysis of The Environment Influencing National Broadband development: A Case Study of Thailand. International Journal of Management, 7(3), 2016, pp. 109–119.

[22] Settapong Malisuwan and Wassana Kaewphanuekrungsi, Analysis of Roadmaps and Trends for Mobile Communication Technology In Thailand. International Journal of Advanced Research in Engineering and Technology, 7(1), 2016, pp. 68-79.

[23] Settapong Malisuwan and Wassana Kaewphanuekrungsi. Analysis of Mobile Telecommunications Market in Thailand International Journal of Management, 6(12), 2015, pp. 01-10.

[24] Settapong Malisuwan, Dithdanai Milindavanij, Wassana Kaewphanuekrungsi and Noppadol Tiamnara, Analysis of Market Competition in Telecommunications Business: Regulatory Perspective, International Journal of Industrial Engineering Research and Development, 7(2), 2016, pp. 31–42.

[25] Settapong Malisuwan, Dithdanai Milindavanij and Jesada Sivaraks, Analysis of ICT Development in ASEAN Countries. International Journal of Advanced Research in Management, 7(2), 2016, pp. 01–10.

[26] Settapong Malisuwan, Dithdanai Milindavanij and Wassana Kaewphanuekrungsi, Analysis of Communication Service in Thailand: A Case Study on the Communication Market 2014 and Outlook 2015. International Journal of Management, 7(4), 2016, pp.158–171.

[27] Settapong Malisuwan, Wassana Kaewphanuekrungsi, Noppadol Tiamnara and Pollawich Apintanapong, A Study of Electromagnetic Radiation Effects From Mobile Phone Base Stations on Human Health. International Journal of Advanced Research in Engineering and Technology, 6(12), 2015, pp. 25-38.

[28] Settapong Malisuwan and Wassana Kaewphanuekrungsi. A Review of Spectrum Auction In 4g Lte 1800 Mhz: The First Transition of Telecommunications Industry From Concessions To Licensing Regime In Thailand, International Journal of Advanced Research in Management, 6(3), 2015, pp. 143-151.

[29] Settapong Malisuwan, Dithdanai Milindavanij, Jesada Sivaraks, Noppadol Tiamnara, A Modified Model of ICT Development Index (IDI) For Thailand To Achieve The ICT Leader In Asean. International Journal of Advanced Research in Engineering and Technology, 6(12), 2015, pp. 39-48.